Homework 02-1 Report

1. Introduction

The goal of this assignment is to build an Agentic AI system capable of automating the Know Your Customer (KYC) compliance process by verifying candidate CVs against public social media profiles on LinkedIn and Facebook. To achieve maximum control over the tool execution process and state management, I bypassed high-level abstractions like AgentExecutor and implemented a Custom Asynchronous Tool-Calling Loop using LangChain and Gemini-2.0-Flash.

2. System Architecture

My implementation consists of a native reasoning loop and a sub-chain extraction mechanism, designed to prevent hallucinations and ensure deterministic output.

2.1 Custom Asynchronous Reasoning Loop (The Core Agent)

Instead of relying on black-box executors, I implemented a robust cv_verification_loop powered by asynchronous iteration (ainvoke). The system manually manages the conversation history, appending human prompts, AI responses, and ToolMessage results at each turn. The loop allows up to 30 reasoning turns, parsing tool_calls directly from the model's response and dynamically mapping them to asynchronous MCP tool executions. This native architecture guarantees absolute transparency and stability in the control flow.

2.2 Structural Extraction Sub-Chain (The read_cv Tool)

To handle unstructured PDF text, I implemented read_cv as an independent @tool. Inside this tool, a dedicated LangChain pipeline (prompt — llm — JsonOutputParser) is used to extract the candidate's name, location, education, and experience into a strict JSON format. The master agent is mandated to call this tool first, ensuring all subsequent MCP searches are based on structured, hallucination-free data.

2.3 Deterministic Scoring Pipeline

To satisfy the binary evaluation metric (threshold at 0.5), the system prompt strictly instructs the model to output a CONFIDENCE_SCORE between 0.0 and 1.0. I implemented a robust Python handler (extract_score) that utilizes Regular Expressions to parse the numeric value from the final report and clamps it safely between 0.0 and 1.0, ensuring mathematically valid outputs for the evaluation script.

3. Implementation Details

The master agent is guided by a strictly defined System Prompt ("MANDATORY WORKFLOW") to utilize the 6 available tools systematically:

Step 1: Extraction: The agent must first invoke the read_cv tool with the raw text to obtain the parsed JSON background.

Step 2: LinkedIn Pass (Primary Verification): The agent invokes search_linkedin_people (using fuzzy matching if necessary) and extracts the person$_idtocallget_linkedin_profile$.

Step 3: Facebook Pass (Secondary Verification): The agent cross-references findings by calling search_facebook_users and get_facebook_profile to detect contradictions in location or current employment.

Step 4: Fraud Detection: The agent actively evaluates profile authenticity. It invokes get_linkedin_interaction to detect "Ghost Accounts" (e.g., senior roles with 0 posts) and uses get_facebook_mutual_friends to verify claimed connections.

4. Evaluation and Sample Results

The system was tested against the 5 hidden evaluation CVs, achieving a perfect 100% accuracy rate (Final Score: 1.0, Decisions: [1, 1, 1, 0, 0]).

Sample 1: Valid CV (CV_1.pdf)

Sample 1: Valid CV (CV_1.pdf)

VERIFICATION_STATUS: VALID

CONFIDENCE_SCORE: 0.7

REASONING: The CV information aligns well with the LinkedIn and Facebook profiles found. The candidate's name, education, skills, and work experience at ByteDance are consistent across platforms.

DISCREPANCIES: The LinkedIn profile indicates that the candidate is a student, while the CV suggests they are currently employed. This could be due to an outdated LinkedIn profile.

Sample 2: Invalid/Fraudulent CV (CV_5.pdf)

VERIFICATION_STATUS: INVALID

CONFIDENCE_SCORE: 0.4

REASONING: The CV states that Rahul Sharma is currently a Senior Engineer at EY, but the LinkedIn profile says he is an Engineer at GreenLeaf Co and a Manager at PwC. The LinkedIn profile also has 0 posts, which is suspicious.

DISCREPANCIES: Current employment on CV (EY) does not match LinkedIn (GreenLeaf Co and PwC). LinkedIn profile has 0 posts. Education on CV (University of Tokyo) does not match LinkedIn (KAIST).

5. Conclusion

By engineering a native, asynchronous tool-calling loop and integrating a JSON-enforced sub-chain for data extraction, the implemented system achieves perfect accuracy on the test set.

The architecture successfully automates the KYC verification process without relying on opaque executor wrappers, demonstrating high stability and deep anti-fraud reasoning capabilities.